Hearing Before the
Committee on the Judiciary
United States Senate

Entitled
"Privacy in the Digital Age: Preventing Data Breaches and Combating Cybercrime"

February 4, 2014

Questions for the Record
Submitted to
The Department of Justice

1. During the February 4, 2014, hearing, you testified about the Department's important work in combating and prosecuting cybercrime. Are there any changes to existing law that would assist the Department in that effort?

Yes, there are several changes to existing laws that would assist the Department in our efforts to combat cybercrime. As an initial matter, we believe that data breach notification legislation, as described further below and in then Acting Assistant Attorney General Raman's written statement at the hearing, is critical to our efforts to protect Americans whose personal information is compromised by cybercriminals. We also have suggested a number of improvements to the criminal laws on which the Department relies in combating cybercrime. One of the most important of those laws is the Computer Fraud and Abuse Act ("CFAA"). It was first enacted in 1986, when the problem of cybercrime was still in its infancy. Over the years, a series of modest changes have been made to the CFAA to reflect new technologies and means of committing crimes, and to equip law enforcement with tools to respond to changing threats. The CFAA has not been amended since 2008, and the intervening years have again created the need for the enactment of modest, incremental changes. The Administration is proposing several such revisions to keep Federal criminal law up-to-date with rapidly-evolving technologies. Many of these proposals are reflected in a bill you recently introduced. For the record, we recap some of these proposals, which are also further described in Ms. Raman's written statement. Finally, we discuss an additional proposal, currently before the Rules Committee for the Federal Rules of Criminal Procedure (Rules Committee), which would improve the process for obtaining warrants to search computers.

Data Breach Notification

Millions of Americans every year are faced with the potential for fraud and identity theft from online breaches of their sensitive, personally identifiable information. The nation clearly needs strong protections for consumers' rights and privacy for sensitive data such as credit card and social security numbers, names and addresses, and medical records. The Administration recommends, as it did in its 2011 proposal, the establishment of a strong, uniform Federal standard requiring businesses to provide prompt notice to consumers and to law enforcement in the wake of a breach of electronic personally identifiable information. Such a law should also

provide for appropriate periods of delay of consumer notification where it would impair a criminal investigation

Deterring Insider Threats

The CFAA addresses the threat posed by insiders – such as employees of a business or of a government agency – by criminalizing conduct by those who "exceed authorized access" to a protected computer. Some have contended that this provision should be limited or abolished because it potentially could be subject to misuse or overuse, such as through the prosecution of people who merely lie about their age when going to a dating site, or harmlessly violate the terms of service of an email provider. In a recent case, an appellate court barred an otherwise meritorious prosecution under the CFAA because of this worry. We are open to working with Congress to assist in developing appropriate statutory amendments, such as new statutory thresholds regarding the value or sensitivity of the information improperly accessed (which would assure that criminal prosecutions could not be brought on the basis of trivial conduct, such as lying about one's age on a dating website), or new language making more explicit that the statute does not permit prosecution based on access restrictions that are not clearly understood.

Access Device Fraud

To ensure that we can prosecute cyber criminals acting overseas who steal data concerning customers of U.S. financial institutions, we also recommend a modification to the access device fraud statute, 18 U.S.C. § 1029. One of the most common motivations for hacking crimes is to obtain financial information. The access device fraud statute proscribes the unlawful possession and use of "access devices," such as credit card numbers. Organized criminal enterprises – often located abroad – have committed such intrusions and exploited the stolen data through fraud that directly affects Americans and United States financial institutions. Yet, under current law, a criminal who possesses or traffics in stolen credit card information issued by a U.S. financial institution, but who otherwise does not take one of certain enumerated actions within the jurisdiction of the United States, cannot be prosecuted under section 1029. The Department recommends that the statute be expanded to allow for the prosecution of offenders in foreign countries who directly and significantly harm United States citizens and financial institutions.

Deterring the Spread of Cell Phone Spying

The Department of Justice recommends the enactment of legislation that would enable law enforcement to seize the profits of those who market and use cell phone spyware. The spread of computers and smartphones in recent years has created a new market in malicious software that allows users to pay a small fee to download sophisticated tools to intercept the communications of unsuspecting victims, such as estranged spouses and business competitors. Selling or using such software is illegal under current law, and current law also provides that courts can order the forfeiture of the surreptitious interception devices themselves. It does not, however, allow for the forfeiture of the proceeds of the sale or use of those devices, or the

forfeiture of any property used to facilitate their manufacture, advertising, or distribution. Further, the surreptitious interception of communications is currently not listed as a predicate offense in the money laundering statute, 18 U.S.C. § 1956. Because perpetrators of these crimes often act from abroad, making it more difficult to prosecute them in the United States, it is particularly important that law enforcement be able to seize the money that the criminals make from engaging in this criminal surveillance and to seize the equipment they use.

Selling Access to Botnets

We also recommend amending current law to better enable the Department of Justice to combat the proliferation of botnets. A botnet is a network of secretly hacked computers, sometimes numbering in the millions, which are located in homes, schools, and offices. Botnets can be used for various nefarious purposes, including the theft of personal or financial information, the dissemination of spam, and cyber attacks, such as Distributed Denial of Service attacks. Federal criminal law already criminalizes the creation of botnets, as well as the use of botnets to hack into other computers or to commit fraud. But those who merely control an existing botnet are not necessarily covered by these laws, nor are those who sell, or even rent, access to the infected computers to others. The Department of Justice recommends that the CFAA be amended to clearly cover such trafficking in access to botnets.

Ensuring Proper Judicial Review of Warrants for Computers

The Department of Justice has previously recommended to the Rules Committee an amendment to Rule 41 of the Federal Rules of Criminal Procedure to update the territorial limits for warrants to search electronic storage media. Currently, Rule 41 does not directly address the special circumstances that arise when officers execute search warrants, via remote access, over modern communications networks such as the Internet. The need for such warrants has increased significantly for at least two reasons.

First, criminals are increasingly using sophisticated anonymizing technologies like proxy services when they commit crimes over the Internet. There are techniques that law enforcement can use to identify a criminal's computer by conducting a remote search of the computer. Yet even when investigators can demonstrate probable cause to believe that the evidence sought via a remote search will aid in the apprehension or conviction of an individual for committing a particular criminal offense, Rule 41 does not explicitly authorize a judge to issue a warrant where law enforcement is unable to identify the district in which the targeted device is located.

Second, criminals are using multiple computers in many districts simultaneously as part of complex criminal schemes, and effective investigation and disruption of these schemes often requires remote access to Internet-connected computers in many different districts. For example, a large botnet investigation is likely to require action in all 94 districts. In some circumstances, search warrants could be used to take action against botnets, but coordinating 94 simultaneous warrants in the 94 districts is impossible as a practical matter.

The Department proposed to the Rules Committee that Rule 41 be amended to authorize a court in a district where activities related to a crime have occurred to issue a warrant for

electronic storage media within or outside the district. While the Department continues to work with the Rules Committee to make this important change to clearly empower courts to review and authorize such warrants, the rules process is a lengthy one. Given the pace of technological change and the urgent need to address this issue, we would welcome Congressional action that could implement this proposal expeditiously.

2. Given the recent trend of "point of sale" data breaches involving United States retailers and the use of so-called "scraping" malware in some of those data breaches, do you anticipate that there will be an increase in this kind of cybercrime involving payment cards in the future?

Yes, the Department has seen and expects to continue to see an increase in cyber attacks on point of sale terminals. The Department's experience with cybercrime has shown two things: (1) cyber criminals will target systems or data that allow them to profit, and (2) cyber criminals have been highly adaptive to changes in cybersecurity practices. Payment card information has long been of interest to financially motivated cyber criminals for the simple reason that the data is valuable. Cyber criminals either use such data in fraud schemes or sell it to others for such use, causing tremendous fraud losses every year. When such data is collected in large databases on retailers' or others' computers, cyber criminals target those databases in order to gain access to the data. As a result of such attacks, many companies have adapted and increased protections for such databases. Today, most stored data containing payment card information is encrypted. As a result, attackers have moved to systems from which useable data may still be collected, most often the point of sale terminals of retailers, where the data valuable to cyber criminals is available in an unencrypted form. As long as valuable data can be gathered from those systems, we expect cyber criminals to continue to try to breach them.

3. During the hearing, you also testified that many of the perpetrators of cyber attacks on United States computers are located outside of the country.

    a. How successful has the Department been at extraditing foreign perpetrators of cybercrime?

Extraditing foreign perpetrators of cybercrime, or any other crime, presents significant challenges. Some countries have laws that prevent the extradition of their nationals. In addition, extradition treaties generally require that both the U.S. and the foreign country have made the conduct a crime; thus, extradition can be very difficult if the foreign country from which we seek the extradition of a criminal has not passed laws that criminalize cyber activities to the same extent as the United States. To deal with these challenges, the Department of Justice, in partnership with the Department of State, develops and provides training to countries to improve their capacity to investigate and prosecute cybercrime and to develop criminal laws harmonized with the laws of the United States and other developed countries. Additionally, the Departments of Justice and State promote worldwide adoption of the Council of Europe Convention on Cybercrime – to which the United States and 40 other countries are parties – which sets up a regime for the criminalization of malicious cyber activities. By establishing a common baseline

of criminal laws, the Convention helps to assure that gaps in foreign countries' laws will not prevent extradition.

Despite these challenges, the Department has worked exceptionally hard to address international cybercrime and, as a result, we have had many successes. Listed below are just some of these successes from quite literally around the world:

- Romania has been an excellent partner in extraditing cyber criminals to the United States. For example, on May 25, 2012, Romania extradited Romanian national Adrian Tiberiu Oprea to stand trial in the District of New Hampshire, where he was charged for his participation in an international, multi-million-dollar, online scheme to hack into U.S. merchants' point of sale computer systems in order to steal their customers' credit, debit, and gift card data. From 2008, members of the conspiracy hacked into point of sale systems at more than 200 point of sale systems throughout the country, compromised over 100,000 credit card accounts, and made unauthorized charges in excess of $17.5 million. Oprea was convicted following his extradition and, in September 2013, was sentenced to serve 15 years' imprisonment.

- In another case, in December 2012, law enforcement officers in Romania, the Czech Republic, the UK, and Canada arrested six Romanians in a coordinated takedown targeting a widespread cyber fraud, passport fraud, and money laundering ring. The suspects were extradited from Romania in March 2013; from the U.K. in July 2013; and from the Czech Republic in the autumn of 2013. All have since pled guilty in Federal court. Extradition proceedings in Canada are pending.

- The Department also successfully extradited defendants from Estonia, South Africa, and France in another major cybercrime prosecution. The case involved the infiltration of the computer system of a credit card processor in Atlanta in which three hackers obtained debit card numbers and decrypted the associated PIN codes. In a 12-hour period, criminals fraudulently withdrew approximately $9.4 million from ATMs around the world.

- In February 2014, the Republic of Georgia, despite the absence of an extradition treaty, used its domestic law to extradite a Turkish national to stand trial in the Middle District of Florida. The fugitive is charged with acquiring stolen credit card numbers obtained from U.S.-based companies by computer hacking. The investigation of this criminal conspiracy has already resulted in 17 convictions in the United States.

- In 2012, a defendant was extradited from Paraguay after his arrest at a hotel, where he was found in possession of counterfeit payment cards and electronic implements to re-encode cards. The defendant had been a fugitive for ten years. He was charged in the District of New Jersey in connection with participation in the "Shadowcrew" forum, an online marketplace for hacking and identity theft. Paraguay extradited him to the United States after he completed a sentence for offenses he committed in Paraguay.

- In 2012, a Russian citizen waived extradition from the Netherlands and was surrendered to stand trial in the District of New Jersey on offenses related to hacking into bank computer networks and subsequently selling stolen debit and credit cards and other personal information.

- In 2012, a Pakistani national waived extradition from the Netherlands and was convicted in the Eastern District of New York of access device charges in connection with orchestrating "unlimited operations" involving intrusions into payment processors and financial institutions, including fraudulent withdrawals of $14 million made within the span of 48 hours in 2011 that targeted the largest payment processor in the world at the time. He was sentenced in 2013.

- In 2013, a Bulgarian national was extradited from Bulgaria to stand trial in a hacking case charged in the District of New Jersey. The case is pending.

- In 2013, a UK national was extradited from the Netherlands, and in 2012, another was temporarily surrendered to face charges that they operated an illicit business in Europe in which they stole point of sale access card reader devices used in commercial establishments and replaced them with non-functional dummy devices and installed "skimmers" in the stolen card readers that intercepted the data from cards swiped through the device and PIN codes entered by the consumer.

- In 2013, Germany extradited a Ukrainian hacker to stand trial in the Eastern District of Virginia.

- In 2013, an alleged hacker was extradited from Thailand to stand trial in the Northern District of Georgia in connection with his role in developing the malicious software SpyEye and also operating a SpyEye botnet.

- In 2012, a Kosovo national was extradited from Germany for his alleged role in a large-scale series of intrusions into payment processors and financial institutions. He is currently being prosecuted in the Eastern District of New York.

- Between 2007 and 2012, thirteen defendants were extradited to stand trial in the District of Connecticut for a "phishing" scheme, which uses the Internet to target individuals and obtain private personal and financial information. Ten were extradited from Romania; one from Bulgaria; one from Canada; and one from Sweden.

- In 2011, a U.S. citizen was extradited from Japan on passport fraud charges to stand trial in the Southern District of California. The defendant was a San Diego IT contractor who stole the personal information of approximately 90 employees and used it to enrich himself. He also made fraudulent statements in order to obtain two different passports.

- In 2011, at the request of the United States, six Estonian nationals were arrested in Estonia on charges of wire fraud and computer intrusion. The arrests were part of a coordinated takedown that included requests for the seizure of financial accounts in several countries. The six are wanted in the Southern District of New York to stand trial for their involvement in a criminal enterprise that infected millions of computers worldwide with malicious software. Two defendants were extradited from Estonia to the United States in 2012.

- In 2009, an Israeli hacker was extradited from Canada to stand trial in the Eastern District of New York on charges involving the orchestration of several intrusions into payment processors and financial institutions. He was ultimately convicted and sentenced in 2011.

- In 2009, a U.S. citizen who fled to Mexico was successfully extradited to stand trial in the District of New Jersey on computer hacking charges.

- In May 2007, an Indian national living in Malaysia was extradited from Hong Kong to stand trial in the District of Nebraska and a second Indian national was extradited from Hong Kong in June 2009. The defendants, while in Thailand and Hong Kong in 2006, had hacked into online brokerage accounts in the United States and operated a "pump and dump" stock fraud scheme that artificially inflated the value of securities. Both defendants pleaded guilty.

While prosecution in the United States for crimes committed here is often our primary goal, we also have worked extensively to encourage prosecutions in those foreign countries where a perpetrator's extradition is not viable and the respective jurisdiction can impose appropriate consequences for cybercrime. We will continue to work with international partners to ensure that justice is done in whatever manner is most appropriate in a given case.

b. Are there any new legal tools that would assist the Department in addressing any obstacles to extradition in cybercrime matters?

The legal tools that Congress has provided to the Department have allowed us to bring prosecutions and, when necessary, successfully extradite defendants in cybercrime matters. Although we are not currently seeking any new legal tools from Congress relating to the extradition of defendants, we continuously evaluate the effectiveness of existing authorities. In addition, we note that in order to secure the cooperation of foreign law enforcement agencies, we need to ensure that the U.S. government can appropriately respond to foreign requests for electronic evidence. The Department's funding for such activities has not kept pace with the dramatic rise in foreign requests, resulting in a backlog. As the President has laid out in his Fiscal Year 2015 budget, substantial additional resources are needed for the Department of Justice to devote to satisfying foreign requests for evidence in cybercrime and electronic evidence cases.